DEPARTMENT OF THE ARMY
Missouri River Division, Corps of Engineers
P.O. Box 103, Downtown Station
Omaha, Nebraska 68101-0103

MRD Regulation
380-1-2 1 January 1987

Security
INFORMATION SECURITY PROGRAM

1. Purpose. To insure that Department of Defense information relating to national security is protected to the extent necessary and to define those administrative procedures required of the Missouri River Division (MRD) staff to implement the information security program.

2. Applicability. This regulation applies to all personnel of MRD who handle classified defense information or may become inadvertently associated with such information. It is not applicable to handling COMSEC material which is covered in separate regulations including MRD-R 380-1-1.

3. References.

a. AR 380-5, and USACE Suppl 1 thereto.

b. AR 380-13, and USACE Suppl 1 thereto.

c. AR 381-12.

d. AR 530-1, and USACE Suppl 1 thereto.

e. AR 604-5, and USACE Suppl 1 thereto.

f. AR 690-1.

g. ER 380-1-12.

h. AR 380-380 and USACE Suppl 1 thereto.

i. AR 530-4 Control of Compromising Emanations (U)

4. Policy. The dissemination of classified information orally, in writing, or by any other means, shall be limited to those persons whose official duties require knowledge or possession thereof and who possess the appropriate level of clearance. No one has the right of access to classified information solely by virtue of rank or position. Accountability and control of classified information will be centralized at Division and District level consistent with operational requirements.

This regulation supersedes MRD-R 380-1-2 dated 1 Oct 84.

5. Security Clearances.

a. Chiefs of divisions and separate offices of the MRD staff will determine those personnel under their supervision requiring a security clearance. Request for a security clearance will be forwarded to the Chief, Security and Law Enforcement, with sufficient justification. Adjudication of the clearance action will be based on the justification provided and the sensitivity of the job position assigned under the provisions of AR 690-1. The servicing personnel office will maintain a record of position sensitivity and provide such information to the Chief, Security and Law Enforcement, upon request. Sensitivity of positions is categorized as follows:

(1) Noncritical-Sensitive. Duties or responsibilities of the position require access to SECRET or CONFIDENTIAL defense information or material.

(2) Critical-Sensitive. Duties or responsibilities of the position may require access to TOP SECRET information or material because of association with war plans, involvement with investigative duties, or other duties demanding the highest public trust.

(3) Nonsensitive. Duties and responsibilities fit neither of the above categories.

b. The Chief, Security and Law Enforcement, is designated as the staff officer to execute DA Form 873, Certificate of Clearance and/or Security Determination, for the Division Commander in accordance with paragraph 1-6c, AR 604-5.

c. Each operating District will have a Security Manager appointed in writing IAW AR 380-5 and USACE Suppl 1 thereto. A copy of each appointment will be furnished to Commander, USACE (DAEN-PMS) and the MRD Chief, Security and Law Enforcement.

d. ENG Form 2410 (Security Clearance Control Card) and SF 189 (Classified Information Nondisclosure Agreement) will be maintained by the Chief, Security and Law Enforcement, on all assigned personnel.

e. Revocation, suspension, and administrative withdrawal of security clearances will be in accordance with AR 604-5.

6. Security Education and Indoctrination.

a. The servicing personnel office for MRD will inform the Chief, Security and Law Enforcement, of the assignment of new employees to MRD or any personnel action effecting a termination, retirement, or transfer. This will be accomplished by routing the Standard Form 50 (Notification of Personnel Action) through the Chief, Security and Law Enforcement.

b. Chiefs of branches and separate offices will:

(1) Insure that block 4E of Standard Form 52 (Request for Personnel Action) is completed accurately.

(2) Continually emphasize to employees the need for protecting classified information.

(3) Indoctrinate personnel fully in the principles, criteria, and procedures for the classification, downgrading, and declassification, including marking, of information as prescribed in AR 380-5.

(4) Familiarize personnel with the specific security requirements of their particular duty assignment.

(5) Advise employees of the hazards involved and the strict prohibition against discussing classified information over the telephone or in such a manner as to be intercepted by unauthorized persona.

(6) Advise personnel of the disciplinary actions that may result from violations of the references at paragraph 3.

c. Indoctrination briefing and debriefing.

(1) Each person granted a security clearance is required to accomplish required reading as outlined on ENG Form 3544 (Personal Security Statement). Supervisors will insure that ENG Form 3544 is completed for each employee, annotated annually and maintained on file in office of assignment.

(2) The servicing personnel office and individual supervisors are responsible for insuring that all cleared personnel departing MRD by transfer, termination, or retirement, report to the Chief, Security and Law Enforcement, for debriefing and execution of DA Form 2962 (Security Termination Statement and Debriefing Certificate).

(3) Prior to assumption of duties, personnel assigned to nonsensitive positions will be indoctrinated thoroughly by their supervisor concerning the basic safeguards and formal principles of the security program. Even though these persons will not have access to classified information in the performance of their duties, it is imperative that they know what action to take should they come in contact with classified information, discover a classified container open and unattended, etc. Indoctrination will be made a matter of record by entering on Standard Form 7-B (Employee Record Card): "Indoctrination under AR 380-5 completed _____(date)_____."

7. Classification Authority.

a. Derivative authority to classify SECRET or CONFIDENTIAL material created as a result of, in connection with, or in response to other material dealing with the same subject matter which already bears SECRET or CONFIDENTIAL classification, is delegated to the following:

(1) Deputy Division Commanders

(2) District Commanders

(3) Chief, Engineering Division, MRD

(4) Chief, Real Estate Division, MRD

(5) Chief, Emergency Management Branch, MOD

(6) Division Administrative Assistant

(7) Chief, Security and Law Enforcement

(8) Chief, Military Program Management Division.

b. District Commanders may sub-delegate the authority as above.

8. Storage and Safekeeping.

a. Classified material will be stored in GSA approved security containers designated for that purpose. Designated containers for MRD will be numbered and maintained within visual contact of the custodian of classified documents or the alternate. Funds, weapons, narcotics, precious metal or any other items of high value will not be stored in a container with classified material.

b. Combinations to security containers will be changed at least every 12 months. Combinations will also be changed immediately upon the transfer, relief, suspension, or separation of an individual having knowledge of the combination. Combinations of containers storing NATO information will be changed every 6 months.

c. Standard Form 700 (Classified Container Information) will be utilized to record a combination.

(1) Part I will be attached to the inside of the container.

(2) Part 2 will be attached securely to the outside of a nontransparent envelope which will be stamped with the highest classification of the material stored in the container.

(3) Part 2A will be stamped with the highest degree classification held by the container, folded,

and inserted into the envelope. The envelope will be sealed, and secured in a GSA approved safe within a designated control office.

d. The tops of security containers will be kept free of all extraneous material. The only items authorized to be on top of a security container are the working copies of Standard Form 702 and Standard Form 701.

e. Standard Form 702 (Safe or Cabinet Security Record) will be forwarded to the Division Security Manager on the day following the last entry.

f. Standard Form 701 (Weekly Security Check Sheet) will be utilized in each office where classified containers are located. The form will be maintained as prescribed in USACE Supplement l to AR 380-5. The form will be forwarded to the Division Security Manager the day after the last entry.

g. Magnetic card OPEN and CLOSED signs will be displayed on the exterior of the containers. The person opening or closing the container is responsible for affixing the appropriate sign.

h. Classified legal size file folders and document covers, Standard Forms 705, 704 and 703, will be stored out of sight when not in use.

9. Inventories. TOP SECRET and NATO SECRET material will be inventoried by the TOP SECRET Control Officer on the first workday in April of each year. This inventory will be witnessed by a disinterested person who has been appointed in writing.

10. Reproduction.

a. The Chief, Security and Law Enforcement, is designated as the authority for all classified reproduction within the MRD staff. District Engineers will designate in writing a responsible individual to authorize reproduction.

b. The designated and marked reproduction machine located in Room 07, 12565 West Center Road, is authorized for the reproduction of classified material under the supervision of the Chief, Security and Law Enforcement.

11. Destruction of Classified Material and Waste.

a. All classified material to be destroyed will be delivered to the Custodian of Classified Documents who will destroy this material using the shredders in Emergency Operations. Material which cannot be shredded will be taken to Offutt Air Force Base for destruction.

b. The Chief, Customer Assistance and Support Branch of Information Management Office, will designate in writing a witnessing official for destruction of TOP SECRET and NATO SECRET material.

12. Emergency Removal or Safeguarding of Classified Information. Planning is necessary to provide for the protection of classified information under emergency conditions such as natural disasters, civil disturbances, and enemy action. See Appendix A, Emergency Removal or Safeguarding Plan for Classified Matter.

13. Subversion and Espionage Directed Against U. S. Army (SAEDA). Pursuant to AR 381-12, AR 380-5, and USACE Supplement to AR 380-5, "SAEDA Orientation" is on file in the MRD Security and Law Enforcement Office to be used as a briefing paper. Specific responsibilities are as follows:

a. When in the continental United States, all individuals will report SAEDA incidents to the Division Security Manager and/or the nearest Intelligence and Security Command (INSCOM) Office. If in a travel status, you may make this report to the nearest FBI office.

b. When traveling outside the continental United States, individuals will report SAEDA incidents to the nearest U.S. military attache, embassy, or consulate, and the Chief, Security and Law Enforcement, upon return.

c. Chiefs of MRD staff elements will:

(1) Insure that all employees under their supervision receive or read a SAEDA orientation annually.

(2) Prepare a listing of their employees' names together with their signatures and dates thereon, signifying that each has read the orientation paper. Listing will be furnished to the Chief, Security and Law Enforcement, within 30 days after the beginning of each calendar year.

(3) Maintain a procedure to insure that all employees hired later receive the SAEDA orientation and instruction at the time of employment and that the Chief, Security and Law Enforcement, is furnished written notification to that effect.

d. Employees traveling OCONUS will receive a Terrorist Awareness Briefing from the Chief of Security and Law Enforcement. It is each employee's responsibility to obtain this briefing.

14. Operations Security (OPSEC). OPSEC is any action taken to enhance or improve the security of that organization, its functions and operations. See Appendix 8, Operations Security Plan.

15. Hand-carrying Classified Material Aboard Commercial Passenger Aircraft.

a. Hand-carrying of classified material aboard commercial passenger aircraft is prohibited unless

properly authorized and only when precautions are taken to preclude inadvertent compromise during pre-boarding screening. This practice will be permitted only in the most extreme cases.

b. Within the United States, its territories and Canada, officials within DOD components who have been authorized to approve travel orders and designate couriers, may approve the escort/hand carry of classified information.

c. Outside the United States, its territories and Canada, the head of a DOD component, or his/her single designee, may authorize the escort/handcarry of classified information. Requests for above authorization must be forwarded through MRDPM to CDR USACE (DAEN-PMS), Washington, DC 20314.

d. Procedures for hand-carrying classified information on commercial aircraft must comply with requirements in paragraphs 8-302 and 8-301, AR 380-5.

16. Acquisition and Storage of Information Concerning Non-Affiliated Persons and Organizations.

a. Chiefs of divisions and separate offices of the MRD staff are required to familiarize themselves once annually with the provisions of AR 180-13, subject above. This will be annotated for record each year and the record will be filed in a policy book maintained by the Chief, Security and Law Enforcement.

b. Chiefs of divisions and separate offices, MRD, will submit an annual report to the Chief, Security and Law Enforcement, attesting that files have been screened and that there is no information in storage that is in violation of AR 380-13. District Security Managers will report the same for their respective elements. Reports will be provided the Chief, Security and Law Enforcement, prior to 15 October of each year.

17. Release of Engineer Information.

a. The Chief, Security and Law Enforcement, will coordinate the release of Engineer information to include (1) all classified and unclassified information to be released to foreign nations or governments and (2) classified information to other United States agencies and citizens.

b. Direct release to requestor of unclassified Engineer information is authorized only as prescribed in ER 380-1-12, para 6.

c. All classified information to be released must be referred to DAEN-PMS. Information to be released must comply with requirements in ER 380-1-12, para 7.

d. Any information to be released, whether classified or unclassified, must be routed through MRDPM.

18. Implementing Instructions. District Commanders will prepare necessary implementing instructions to effectively carry out the policies of the Information Security Program. Implementing instructions should not necessarily duplicate those already outlined in other directives unless further clarity is desired or organization and operational requirements dictate. A copy of district implementing instructions will be furnished the Chief, Security and Law Enforcement.

FOR THE COMMANDER:

/s/
Lee W. Tucker
Colonel, Corps of Engineers
Deputy Commander

2 Appendices
Appendix A - Emergency Removal
or Safeguarding Plan for
Classified Matter
Appendix B - Operations Security
Plan (OPSEC)

DISTRIBUTION:
MRO - A&B
MRK - A
MRD - 15

APPENDIX A

EMERGENCY REMOVAL OR SAFEGUARDING PLAN FOR CLASSIFIED MATTER

1. Purpose. To provide for emergency removal or safeguarding of all classified matter at MRD should civil disturbance, disaster, or enemy action so require.

2. Applicability. These procedures are applicable to all staff elements of MRD.

3. General. AR 380-5 does not authorize the destruction of classified information under emergency conditions in CONUS. Actions contemplated by this plan include only securing the material in authorized containers or removing it from the headquarters.

4. Responsibilities.

a. During normal duty hours, the custodian or alternate custodian wilt perform the necessary actions. After duty hours, personnel listed on DA Form 727 (Classified Container Information) posted in front of Room 39, Emergency Management Branch, will be expected to report to MRD, upon notification, to take necessary action.

b. District Security Managers will develop emergency removal or safeguarding plans and forward a copy to the Chief, Security and Law Enforcement.

5. Implementation. In case of an emergency requiring such action, office chiefs will be directed to return any classified material to the repository of classified documents (Room 39). Further instructions will be issued depending on the type and severity of the emergency. The following conditions and procedures apply to the removal of classified material from files.

a. Emergency removal of classified material from files will be implemented only when directed by the Division Commander, or in that individual's absence, the Chief, Emergency Management Branch, or the Chief, Security and Law Enforcement. Such actions would be directed under Condition BRAVO, which is defined in MRD Continuity of Operations Plan (COOP). Such action could also be directed in the case of natural disasters or civil disturbances which constitute a threat to the security of classified information.

b. Transportation and personnel required for the movement of classified files will be provided by the Customer Assistance and Support Branch of the Information Management Office.

c. The adequacy of protective measures for files being transported will be determined by the Chief, Security and Law Enforcement.

APPENDIX B

OPERATIONS SECURITY (OPSEC) PLAN

1. Purpose. To provide guidance for the protection of sensitive and classified information concerning the normal everyday activities and procedures involved in the accomplishment of MRD's civil and military missions.

2. Applicability. This appendix applies to all personnel assigned to the Missouri River Division, US Army Corps of Engineers.

3. Threat Analysis.

a. Operations Security (OPSEC) is any action taken by a military organization or its contractors, which enhances or improves the security of that organization, its functions or operations. OPSEC relies on policies and procedures which are geared to stop the enemies of the United States from procuring information concerning our military capabilities or vulnerabilities. OPSEC should also prohibit attempts of sabotage, espionage, terrorism or destruction of government facilities, programs or operations.

b. A viable OPSEC program consists of personnel, document, physical, signal, imagery and information security programs. The OSPEC Program is oriented toward countering the threat posed by the enemies of the United States.

c. The threat posed by enemies of the United States to the mission of the Missouri River Division pertains to all division activities which ensure the safety and security of the environment, civilian and military activities and the inhabitants of the division’s area of responsibility.

d. Such division responsibilities as flood control, hydro-electric power, dams, bridges, river traffic, etc., impact upon the normal activities of all inhabitants of the area and the daily functions performed within this area. The control of resources and activities will be essential to the timeliness of mission completion.

e. The CONUS sustaining base consists of all activities, which normally occur during peacetime and which become essential to support tactical operations during wartime. These activities cut across the spectrum of American industry, including subsistence, transportation, communications, as well as military training facilities.

f. MRD’s geographical area is vulnerable to disruption of normal Corps of Engineers functions. Modification of many Division functions could have serious impacts upon the area of responsibility.

4. The Threat. The most serious threats to the security of any MRD operation or activity are hostile intelligence services (HOIS) and their agents. OPSEC activities counter these threats which are human intelligence (HUMINT), signal intelligence (SIGINT), and imagery or photographic intelligence (IMINT). In the Missouri River Division, the threat relates to such civil works functions as locks and dams, hydropower plants, DOD emergency facilities and critical technology items under construction. Military construction targets include design, contracting, inspections, and operations of critical technology items under construction.

a. HUMINT Threat. The HUMINT threat involves acquisition of information by enemy agents concerning tactical and strategic military capabilities and intentions. Within the Corps of Engineers, the HUMINT threat is directed against either military construction or civil works.

b. SIGINT Threat. The SIGINT threat is against all U.S. communications systems. It includes communications intelligence (COMINT) and electronic intelligence (ELINT).

c. IMINT. IMINT is the use of photographic equipment to gain information. IMINT is primarily used by aircraft with infrared and other photo devices or by airborne platforms such as satellites.

5. Countering the Threat. Security programs such as physical security, information/personnel security, and signal security counter the hostile intelligence threat by protecting classified information and educating personnel in techniques to preventing unauthorized disclosures of such information.

a. HUMINT threat is countered by adhering to physical security and information security practices as defined in AR 190-13 and AR 380-5.

(1) Physical security measures include, but are not limited to, the use of security guards, working dogs, restricted areas, perimeter barriers, protective lighting, security containers, locking devices, intrusion detection systems, and access control systems.

(2) Information/personnel security procedures are designed to protect classified and unclassified material which, if analyzed by hostile intelligence agencies, might yield usable intelligence.

b. The SIGINT Threat is countered by adherence to sound signal security (SIGSEC) practices. SIGSEC includes communications security (COMSEC) and the control of compromising emanations (TEMPEST). While one item of information may not be classified, a collection of such information might be and, therefore, should be protected. In such instances, the item of information should be marked “FOR OFFICIAL USE ONLY”. Under no circumstances will any classified information be disseminated over

over the telephone or other nonsecure means. A secure telephone is available in Room 39. TEMPEST hazards must be considered when ordering new signal and ADP equipment.

6. Responsibilities.

a. The OPSEC point of contact (POC) at each district is the Security and Law Enforcement Manager, and at MRD, the Chief, Security and Law Enforcement. The OPSEC POC will insure that periodic OPSEC security awareness briefings are conducted in accordance with AR 530-1.

b. All supervisors are responsible for insuring that their personnel hold security clearances appropriate to the requirements of their duties.

c. Each employee assigned to MRD and subordinate activities is responsible for insuring that all aspects of the OPSEC program are practiced continuously.

d. MRD activities will not hold, approve, or sponsor any meetings off government installations or outside cleared facilities of DOD contractors in which classified information is disclosed. The release of any information, especially classified information, to civilian contractors must be scrupulously controlled. Dissemination of classified information will be made on a strict need to know basis with personnel who have appropriate clearances.

e. All dams, hydroplants, major flood control works, navigation projects, and test sites at MRD operated facilities will have OPSEC plans. These OPSEC plans will determine the sensitivity aspects of the operation, analyze the risk, and determine countermeasure requirements.

f. The Division Automation Systems Security Manager (SSM) is responsible for oversight of the ADP Security Program. The policies prescribed by AR 380-380 and its USACE supplement must be followed at all times.